DEFCON 22 Postmortem Trip Report

August 7, 2014

Edward Fok, FHWA/OTS Resource Center, San Francisco, CA
Ray Murphy, FHWA/OTS Resource Center, Matteson, IL

Overall Theme = Infrastructure vulnerabilities, vehicle hacking, proliferation of advanced hacking tools.

Summary:

- Field network and roadside infrastructure continues to be an area of interest to the hacker community. A number of sessions focused on hacking wireless roadside sensors, limited ride transit cards, 911 systems, and municipal wireless networks. These vulnerabilities do not represent identification of new technical flaws, but a result of poor network management practices by operating properties and manufacturers.
- Vehicle hacking continues to be an area of interest but work has slowed down. This is could be due to a combination of difficulties involved and other demands on the primary investigator's time.
- The hacker tool box continues to expand. A number of sessions and demonstrations of amateur/hobbyist software defined radios. The availability of these tools effectively ends any protection offered by licensed, obscure, or private spectrums between 100MHz and 6GHz.
- The hacker community also shows significant interest in a series of NSA tools revealed in documents leaked by Edward Snowden. These are very powerful attack tools that can be utilized by Group 2 or Group 3 attackers.
- This is the first year of a full time Industrial Control System Hacking Village. A simulated control system was assembled to allow participant to attack the controllers using various techniques. This is a similar setup to the training facility used by ICS-CERT in their industrial control system classroom. There are increasing level of interest to industrial control systems and we should not be surprised to see devices from the transportation industries represented in future hacking villages.
- A recurring theme expressed in many sessions, by convention organizers and hacker thought leaders, on the inability of network defender to keep pace with attackers. This change in mindset should be monitored as it could develop tools, processes, and allies that could help us accomplish our mission objectives.
- The size of the conference is growing. The amount of coverage was possible only with planning and coordination with other staff members in attendance. Significant benefit was gain in expanding the state of awareness from discussion with participant from other modes and agency partners.

Hacking Traffic Control Systems

The security researcher at IoActive presented his work on hacking Sensys wireless vehicle detector. The vulnerability allows an attacker to simulate over-count, under-count, fakes data injection, or renders the detector inoperable at a detector station. This attack must be aimed at a detector's wireless access point and a single attacker cannot manipulate detector data across multiple access points simultaneously.

From our meeting with the researcher he failed to show any attempt or demonstrate any ability to push past the field access point used by the detectors.

Program area impacted:

Arterial and Freeway Operations – this reinforces our emphasis for a proactive operating and maintenance program. Proactive programs will recognize the abnormal data generated by this type of attack and can be mitigated using existing respond to failed detection systems. Central systems can use error checking techniques to identify bad data generated from detector access point hacking. Our partner agencies should

be aware of these vulnerability and capabilities of their own system in order to adapt their operation or purchasing decision according to their risk tolerances.

Vehicle Hacking

Researcher in the area developed a metric to rate vulnerabilities of vehicles to cyber-attacks. The rating is based on the vehicle network architecture and OEM could benefit from incorporating the lessons into future designs. The researchers introduced a proof of concept of an Intrusion Prevention System for vehicle network. Without examining it in detail it is unclear how well it will work across the spectrum of possible attacks. However, this is a positive developing from this vulnerability research.

There should be new results next year about the vulnerability of vehicle to remote wireless attacks.

Program Area Impacted:

NHTSA could find this information useful if they choose to assess vehicle resiliency. NHTSA Staff were on hand during the session and are fully aware of the researcher's findings.

Proliferation of Software Defined Radio as an exploit tool

A Software Defined Radio (SDR) is a radio that can change its behavior using software. A single piece of hardware can be a WiFi Radio, a Bluetooth Radio, or a public safety radio depending on the software running on the chip. Multiple sessions described the use of customizable to exploit vulnerabilities in Radio Frequency Identification (RFID)

Program area impacted:

Connected Vehicle, operations, automated vehicle – this could potential increase the likelihood of previously 'private' wireless network be exposed to attacks. Proliferation of these tools completely negates any security benefits of licensed radio frequencies.

Transit Card Hacking

Researchers presented their work on how to hack transit ticket systems that uses the MiFare Ultralights cards. They uncovered new security vulnerabilities that allow them to timestamp the transit ticket with an NFC-enabled Android phone (Near Field Communication - a wireless connectivity technology that enables convenient short-range communication between electronic devices) and turn a limited-ride ticket into an unlimited one; causing potential loss of revenue to transit agencies. The tickets are MiFare Ultralights, http://www.mifare.net/products/mifare-smartticket-ics/mifare_ultralight/ and are used in many major cities around the world. The NFC technology is becoming more widespread; a host of US cities whose transit systems rely on it, including Boston, Seattle, Salt Lake City, Chicago and Philadelphia. To date, vulnerability attack testing (hacking MiFare Ultralight card usage) has only been performed on the Muni system in San Francisco and New Jersey, with its Path transit system. The agencies cited may not be the only ones using cards based on this technology.

Program Area Impacted:

None in Federal Highway Administration - Federal Transit Administration or Federal Rail Administration programs

Here are some of the technical steps identified during the session that could Mitigating the vulnerabilities:

- Implement a firmware update on the stamping machines that would program them to refuse to validate a locked ticket.
- The only solution regarding the date-change hack is to encrypt all data on the ticket.
- With the MiFare Ultralights typically not being encrypted, agencies should request some level of encryption from the manufacturer.

Municipal wireless network hacking

Municipalities across the nation are deploying IP-based 802.11 wireless mesh networks for city-wide services, including cameras and microphones for police monitoring, and remote audio broadcasting. This research examined a deployed and operational municipal mesh network using proprietary wireless mesh protocol. The researchers demonstrated decoding/hacking the police department's wireless mesh network/protocol and were able to "tune in" to live feeds from the various cameras positioned across the city and (2) inject arbitrary/bogus video into these streams. They found that there was almost no security and could be accessed by anyone; a rogue network could request all cameras. Wi-Fi signals were completely unencrypted and names of equipment makers were printed on network boxes, saving time for potential attackers looking for known vulnerabilities. In addition, there were diagrams mapping the mesh network and its functions, including cameras on the municipal website. Municipal managers need to consistently implement commonly accepted best practices for network management and configuration.

Program area impacted:

Any USDOT program relying on partner infrastructure: There are many USDOT and FHWA operations program which relies on communication infrastructure managed by our partners at the state and local agencies. Wireless network continues to be a cost effective solution to some connectivity challenges, but they should be better managed. Many of these agencies continue to demonstrate a lack of proficiencies in securing their wireless network. This could cause reliability and resiliency issues that could affect project performance, on budget, and on time delivery. This is an area where we could develop guidance to program and Division office to enhance oversight in this area.

911 System Hack

Researchers presented their results on investigating potential vulnerabilities across the entire 911 system and detailing current attacks being carried out on 911 systems. The goal of the hack was to initiate emergency response when not appropriate, interrupt/interfere emergency services (911 responses) and gain access of 911 system surveillance. Disruption attacks including cell phone jamming, Automated Location Information (ALI) database editing, TDoS (Telephony Denial of Service) attacks targeting essential public services and resource exhaustion (both virtual & personnel). It should be noted that potential damage extends beyond individuals not being able to talk to 911; i.e. life or death in delaying medical emergencies, etc. 911 systems should implement hardening techniques from IT industries. Primarily basic network protection (such as use of anti-virus software) and response plan in case of cyber incidents.

On April 10th 2014, an estimated 4,500 emergency calls made in Washington state during a 911 call dispatch systems outage (CenturyLink network) failed to reach 127 local emergency call centers within a 6 hour timeframe. The emergency centers in Washington State are interconnected; so when a network outage occurs it can take them all down at once. The target was the ALI database.

Program area impacted:

Emergency related programs under operations: Program and guidance material should include discussion of how operations could coupe if 911 systems become unavailable during an emergency event.